Kiegészítés az Algebra 1 vizsgatételeihez

(6) **Definíció**. Akkor mondjuk, hogy egy G csoport előáll A és B részcsoportjainak (belső) direkt szorzataként, ha

- A és B a G normális részcsoportjai,
- $A \cap B$ csak a G egységelemét tartalmazza,
- A és B együtt generálják G-t.

A fentivel ekvivalens definíció:

Definíció. Akkor mondjuk, hogy egy G csoport előáll A és B részcsoportjainak (belső) direkt szorzataként, ha

- G minden eleme előáll egyértelműen egy A-beli és egy B-beli elem szorzataként,
- $ab = ba$ teljesül minden $a \in A$ és $b \in B$ elemre.

Csoportok külső direkt szorzata. Legyenek A és B csoportok. Az $A \times B$ Descartes-szorzaton definiáljunk műveletet úgy, hogy tetszőleges $a_1, a_2 \in A$ és $b_1, b_2 \in B$ esetén legyen $(a_1, b_1)(a_2, b_2) = (a_1a_2, b_1b_2)$. $A \times B$ erre a műveletre nézve csoport, amelyben (e_A, e_B) az egységelem (itt e_A az A csoport, e_B a B csoport egységeleme), és egy (a, b) elem inverze (a^{-1}, b^{-1}). Ezt a csoportot az A és B csoportok külső direkt szorzatának nevezzük.

A belső és külső direkt szorzat közötti kapcsolat: Az A és B csoportok külső direkt szorzatában az (a, e_B) alakú elemek egy olyan A' részcsoportot alkotnak, amely izomorf A-val, az (e_A, b) alakú elemek pedig egy olyan B' részcsoportot, amely izomorf B-vel. Egyszerűen belátható, hogy az $A \times B$ csoport az A' és B' részcsoportok belső direkt szorzata. Ha az egymással izomorf csoportokat azonosítjuk egymással, akkor azt is lehet mondani, hogy az A és B csoportok $A \times B$ külső direkt szorzata megegyezik a belső direkt szorzatukkal.

Az is megmutatható, hogy ha egy G csoport előáll A és B részcsoportjainak belső direkt szorzataként, akkor G izomorf az A és B csoportok külső direkt szorzatával. Itt G egy g elemének azt az $(a, b) \in A \times B$

elempárt feleltetjük meg, amelyekkel g előállítható egyértelműen $g = ab$ alakban.

Definíció. (Belső szemidirekt szorzat). Akkor mondjuk, hogy egy G csoport előáll A és B részcsoportjainak (ebben a sorrendben vett) belső szemidirekt szorzataként, ha

- B a G normális részcsoportja,
- A és B metszete csak a G egységelemét tartalmazza,
- A és B együtt generálják G-t.

Tétel Egy G csoport tetszőleges A részcsoportja és tetszőleges B normális részcsoportja esetén az alábbi feltételek egymással ekvivalensek.

- G az A és B (ebben a sorrendben vett) belső szemidirekt szorzata.
- G minden eleme egyértelműen előáll ab alakban egy A-beli a és egy B beli b elemmel.
- G minden eleme egyértelműen előáll ba alakban egy B-beli b és egy A beli a elemmel.

Definíció. (Külsö szemidirekt szorzat) Legyenek A és B csoportok, és legyen φ az A csoportnak a B csoport $AutB$ automorfizmuscsoportjába való homomorfizmusa; a B csoport $\varphi(a)$ automorfizmusának B valamely b elemére való hatásásaként adódó elemet jelölje b^a. Az A és B csoportok $A \times B$ Descartes szorzatán definiáljunk egy műveletet a következőképpen: tetszőleges $(a_1, b_1), (a_2, b_2) \in A \times B$ párokra legyen

$$(a_1, b_1)(a_2, b_2) = (a_1 a_2, b_1^{a_2} b_2).$$

Az így keletkezett algebrai struktúra csoport, amelyet az A és B csoportok külső szemidirekt szorzatának nevezünk.

Tétel Ha egy G csoport előáll egy A részcsoportjának és egy B normális részcsoportjának belső szemidirekt szorzataként, akkor A-nak B automorfizmuscsoportjába való azon φ leképezés, amely A tetszőleges a eleméhez B elemeinek a-val való konjugáltjait rendeli, homomorfizmus. Továbbá G előáll az A-nak és B-nek ezen $\varphi : A \mapsto Aut(B)$ homomorfizmussal definiált külső szemidirekt szorzataként.

(8) **Tétel** Ha $n \geq 3$, akkor az S_n szimmetrikus csoportban minden páros permutáció előállítható 3 hosszúságú ciklusok szorzataként, azaz az A_n ($n \geq 3$) alternáló csoportot generálják a 3 hosszúságú ciklusok.

Bizonyítás. Legyen $n \geq 3$. Tudjuk, hogy S_n-ben minden permutáció előáll transzpozíciók szorzataként. Azt is tudjuk, hogy egy permutáció akkor és csak akkor páros, ha páros sok transzpozíció szorzataként állítható elő. Ezért, ha egy permutáció páros, akkor az előállításában szereplő transzpozíciókat párosthatjuk (az elsőt a másodikkal, a harmadikat a negyedikkel, stb ...). A transzpozíciópárok szorzata vagy $(a\,b)(a\,c)$ alakú, vagy (a b)(c d) alakú (itt a, b, c, d páronként különbözőek). Belátható, hogy

$$(a\ b)(a\ c) = (a\ b\ c)$$

és

$$(a\ b)(c\ d) = (a\ b\ c)(a\ d\ c), \quad \text{ha} \quad n \geq 4,$$

amiből már következik a tétel állítása.

(10) **Tétel** Véges G csoport adott p prímhez tartozó p-Sylow részcsoportjainak metszete a G csoport normális részcsoportja.

Bizonyítás. Sylow 3. tétele szerint, ha egy véges G csoport összes különböző p-Sylow részcsoportjai $H_1, \ldots, H_k$, akkor bármely H_i ($i = 1, \ldots, k$) p-Sylow részcsoportnak G tetszőleges g elemével való $g^{-1}H_ig$ konjugáltja is p-Sylow részcsoport. Nyílvánvaló, hogy $g^{-1}H_ig = g^{-1}H_jg$ akkor és csak akkor teljesül, ha $i = j$. Ezért van olyan k-adfokú σ permutáció, melyre $g^{-1}H_ig = H_{\sigma(i)}$ teljesül ($i = 1, \ldots, k$). Így $\cap_{i=1}^k H_i = \cap_{i=1}^k H_{\sigma(i)}$. Legyenek $g \in G$ és $a \in \cap_{i=1}^k H_i$ tetszőleges elemek. Mivel $a \in H_i$ minden i indexre, ezért $g^{-1}ag \in \cap_{i=1}^k H_{\sigma(i)} = \cap_{i=1}^k H_i$. Tehát a $\cap_{i=1}^k H_i$ metszet minden elemének G tetszőleges elemével való konjugáltja is eleme a $\cap_{i=1}^k H_i$ metszetnek, amiből következik, hogy G összes p-Sylow részcsoportjainak $\cap_{i=1}^k H_i$ metszete normális részcsoportja G-nek.

(11) Egy G csoport részcsoportjainak

$$G = G^{(0)} \rhd G^{(1)} \rhd \ldots G^{(i-1)} \rhd G^{(i)} \rhd \ldots$$

sorozatát a G csoport kommutátorláncának nevezzük, ha $G^{(i)}$ a $G^{(i-1)}$ kommutátor részcsoportja minden $i = 1, \ldots$ indexre.

(12) **Tétel**. (Burnside-tétel) Ha a G csoport rendje $p^n q^m$, ahol p és q prímek, akkor G feloldható.

Tétel. (Feit–Thompson-tétel) Minden páratlan rendű csoport feloldható.

Tétel. Egy G csoport akkor és csak akkor feloldható, ha kommutátorlánca leér a G egységeleméig.

(14) **Kis elemszámú csoportok**

Használni fogjuk a következő tételt.

Tétel 1 *Ha G egy $2p$-rendű csoport, ahol $p > 2$ prím, akkor G izomorf a $C(2p)$ ciklikus csoport és a D_p diédercsoport közül az egyikkel.*

Bizonyítás. Legyen G egy $2p$-rendű csoport, ahol p egy 2-nél nagyobb prínszám. A Cauchy-tétel alapján tudjuk, hogy G-nek van olyan f és t eleme, melyre $o(f) = p$ és $o(t) = 2$. Az f elem által gerált F részcsoport izomorf a $C(p)$ ciklikus csoporttal. Mivel F indexe 2, ezért F normális részcsoportja G-nek. A t elem által generált T részcsoport izomorf a $C(2)$ csoporttal. Továbbá, $F \cap T = \{e\}$, ahol e jelöli a g egységelemét. Így $|G| = |FT|$. Ha t felcserélhető f-fel, akkor G kommutatív, és ekkor $G = F \times T \cong C(p) \times C(2)$. Mivel $(2, p) = 1$, ezért G ciklikus csoport. Vizsgáljuk azt az esetet, amikor $ft \neq tf$. Ekkor G elemei $e, t, ff^2, \ldots, f^{n-1}, tf, tf^2, \ldots, tf^{n-1}$, azaz $G \cong D_p$. $\square$

Izomorfiától eltekintve, az alábbi (legalább két, de legfeljebb tíz elemet tartalmazó) kis elemszámú csoportok léteznek:

- Egyetlen kételemű csoport van: ez a $C(2)$ ciklikus csoport.
- Egyetlen háromelemű csoport van: ez a $C(3)$ ciklikus csoport.
- Mivel a négyelemű csoportok mindegyike kommutatív (mert minden p^2 rendű (p prím) csoport kommutatív), ezért két négyelemű csoport létezik a véges kommutatív csoportok alaptétele szerint: az egyik a $C(4)$ ciklikus csoport, a másik a $C(2) \times C(2)$ csoport.
- Egyetlen ötelemű csoport van: ez a $C(5)$ ciklikus csoport.
- Két hatelemű csoport van a Tétel 1 szerint: az egyik a $C(6)$ ciklikus csoport, a másik a D_3 diédercsoport.
- Egyetlen hételemű csoport van: ez a $C(7)$ ciklikus csoport.

- Öt nyolcelemű csoport van. A kommutatív nyolcadrendűek: a $C(8)$, a $C(4) \times C(2)$ és a $C(2) \times C(2) \times C(2)$ csoportok. A nem kommutatív nyolcadrendűek: a D_4 diédercsoport és a Q kvaterniócsoport. A 8 elemű csoportról először is kimutatjuk, hogy – ha nem kommutatív – van negyedrendű eleme. Általában igaz ugyanis az, hogy ha egy csoport minden eleme másodrendű, akkor a csoport kommutatív. Valóban, ha $a^2 = b^2 = (ab)^2 = 1$, akkor ba = 1ba1 = aababb = a(ab)2b = a1b = ab. Így a kérdéses csoportban van egy negyedrendű a elem. Ha $b \notin < a >$, akkor $< a, b >$ rendje nagyobb, mint négy, tehát ez az egész csoport. Mivel a centrum szerinti faktorcsoport nem lehet ciklikus, ezért $< a >$ képe ebben a faktorcsoportban nem lehet az egész csoport. Ez azt jelenti, hogy $< a >$-ban van az e egységelemtől különböző centrumelem, ami csak a^2 lehet, mert a centrumnak nem lehet négy eleme. Mivel a csoport nem kommutatív, ezért generátorelemeik nem felcserélhetőek. Így az $[a; b] = aba^{-1}b^{-1}$ nem az egységelem. A centrum szerinti faktor azonban kommutatív, így a fenti kommutátor benne van a centrumban, azaz $aba^{-1}b^{-1} = a^2$. Ebből azonnal adódik a $ba = a^3b$ összefüggés. Ha $b^2 = e$, akkor a kapott csoport nyilván D_4 lesz. A másik lehetséges eset az, hogy $b^2 = a^2$ amikor az úgynevezett kvaterniócsoportot nyerjük.
- Két kilencelemű csoport van (mivel a p^2 (p prímszám) rendű csoportok kummutatívak): a $C(9)$ ciklikus csoport és a $C(3) \times C(3)$ csoport.
- Két tízelemű csoport van a Tétel 1 szerint: a $C(10)$ ciklikus csoport és a D_5 diédercsoport.